DRAFT

Plan for State Wide Area Network VLAN and IP Address Standardization

Prepared by Brenda Hulphers, Transport Planning

4/20/2004

Executive Summary

The State of Utah Information Technology Services Division (ITS) provides wide area network (WAN) connectivity for executive branch of government agencies. ITS currently uses 5 Class B IP (Internet Protocol) addresses acquired from the Internic to meet the addressing requirements for state agencies. ITS is also currently allowing selected private IP addresses to be routed within the internal State WAN. The philosophy and assignment of IP addresses to state agencies has evolved over the course of a number of years. When the IP protocol was originally introduced into the state WAN, the state network was organized into specific geographic areas because of the requirements of the OSPF (open shortest path first) routing protocol being used at that time. The state WAN was later redesigned to point most remote state agency locations into a central headquarters location for that agency. At that time, ITS shifted the IP philosophy to assign contiguous IP address blocks from specific ranges to individual agencies where possible. Most recently, the Transport Planning group has been redesigning the WAN to point remote locations into geographic hub locations that provide redundant paths to the two state data centers in Salt Lake City and Richfield. The redundant paths are built on both public carrier networks and the private state microwave network. ITS Transport Planning is now in the process of examining the current IP assignment philosophy and making recommendations for changes based on the WAN redesign project, ease of management, flexibility, and for reporting and security purposes. This plan will detail the new philosophy as proposed by ITS Transport Planning. The key components will involve assigning a combination of public and private IP addresses to meet state agencies' needs, a standardized numbering scheme for implementing VLAN (virtual local area network) technology, and access control lists (ACLs).

Details of Proposed Plan

ITS Transport Planning recognizes that, as the demands of both new technologies and applications expand, the Wide Area Network must be capable of supporting varied and sometimes conflicting demands. ITS Transport Planning must present a plan both for agencies and for internal use that will be flexible enough to accommodate changes in traffic priority, technological directions and growth. One area where change is required to support the future is in the way that IP addresses are managed and distributed. A key component of this design requires a well-defined scheme for implementing VLANs throughout the network. This plan will present a standard for creating VLANs and a numbering scheme for managing and controlling them. The implementation of this plan will result in:

- A standardized numbering scheme for VLANs so that each VLAN number assigned by ITS will have a unique meaning and be easily recognizable as to what it represents throughout the network. The numbering scheme will be flexible enough to accommodate various agency requirements, services, applications, and other special circumstances.
- A plan for segregating ITS managed equipment in one or more separate VLANs so that access can be more easily secured and controlled. This plan will make use of a block of public IP addresses set aside for the purpose of standardizing IPs assigned for the installation of new ITS managed equipment.

- Plans to identify who requires access to the ITS managed equipment and to build appropriate access control lists (ACLs) to implement the security required to control access to ITS equipment.
- A plan to provide each agency with a VLAN numbering scheme to accommodate the use of both public and private IP address ranges that will be routed through the WAN (172.X.X.X as per Appendix A).
- A plan to retroactively apply this numbering scheme to the existing ITS assigned VLAN structure already in place across the WAN.
- This plan applies only to VLANs assigned by ITS. It doesn't apply to campus environments behind agency firewalls or an agency's own equipment where the agency has created its own internal VLAN numbering scheme.
- VLANs will be incorporated into the standard WAN product where the creation and application of VLANs are not limited by equipment capabilities or other technological restrictions.
- Timing of upgrades will occur over the normal replacement schedule based on end of life cycles for network equipment.
- VLANs may never be offered in certain locations based on the type of network connectivity.

Implementation of this project will require coordination with several other ITS projects, including the creation of inside and outside DNS service, setup of CiscoWorks product family, setup of Cisco ACS, and the ongoing installation of routers and switches capable of running VLANs at agency locations around the state.

In general, public IP addresses are distributed according to a scheme where each agency has been assigned a large block of IP addresses from within one of the state's class B address ranges. ITS Transport Planning will continue to maintain control of how these blocks are assigned to various agency locations. While there are instances where this model has not been strictly followed or where technological limitations prevent implementation of this model (i.e., non-state agencies or multiple agencies at one location that share a common block of IPs), this plan recommends that ITS Transport Planning continue to follow this model where practical for public IP address assignments. Agencies sharing subnets at a single location will also be separated into their own subnets and VLANs as soon as financially possible. This will require some rework on the part of the agencies, but most have indicated through the WAN Users Group that they are willing to make changes that will help standardize the network. This may also enable ITS Transport Planning to use VLANs or IP address blocks as a means of tracking bandwidth usage for any imaginable purpose at some time in the future.

Note: Assigning IP addresses to maximize IP routing summarization is no longer a concern due to newer technology.

1) Creation of VLAN specifically for ITS managed equipment

ITS Transport Planning will use VLAN 3 to manage and secure ITS owned equipment. The intent is to keep ITS equipment segregated from other agencies' equipment and to control who has access to the ITS equipment. VLAN 3 has already been deployed in the WAN for this purpose. At the present time, this VLAN will include both IP-enabled network equipment and management of telephony equipment. Transport Planning will assign all VLAN 3 IP addresses from a reserved range of public IP addresses designated specifically for this purpose. See Appendix A for details. This plan will also be retroactively applied to remote locations over time where technology to support VLANs is available. ITS Transport Planning will reserve other VLANs for future use within the division.

2) Access Control Lists (ACLs)

Access control lists will be applied for modularity / segmentation reasons to control who has access to ITS and agency owned and managed equipment. For agency personnel that need access to specific ITS owned equipment, ITS will conduct a collaborative effort with representatives from those agencies to design access lists that are tightly enough controlled to provide effective security, but flexible enough to allow the agencies the access that they need to perform their responsibilities or gather the information that they need. The ITS Review Team (Transport Planning, Security, Network Operations, etc.) will review ACL requests prior to implementation to insure that their application will produce the intended results.

Agencies will be able to request that ITS apply specific ACLs to VLANs created for their own local network security requirements. Only one access control list can be applied to a VLAN.

3) Network Management Tools

ITS will use network management tools such as Cisco Works and Cisco ACS to control access to ITS owned network equipment in VLAN 3. These tools will enable ITS personnel to control not only who has access to ITS routers and switches, but to control what people can do once access is granted and to log changes as required. These levels of access will be controlled by Transport Planning and established according to carefully designed parameters that are supported by the IT directors and staff from each agency. ITS plans to allow agency access to network management tools on a per needed basis.

4) Standardized Numbering Scheme for Agency VLANs/ Other Products & Services/ Applications

This plan defines the standardized numbering scheme that will apply to all agencies across the WAN (Appendix B). The plan also defines a block of VLAN numbers reserved for specific ITS services and applications (Appendix C). Each agency will be provided with their choice of a public or private VLAN per each remote location, or both. This plan recommends that the public VLAN be used by agencies primarily for servers that will be open to the Internet outside of the protected state WAN. VLAN numbers can be up to 4 digits long. Certain VLAN numbers are reserved for vendor use on network equipment.

ITS Transport Planning will assign private IP addresses from the pool created for each geographic hub location using 172.X.X.X IP addresses (Appendix A). In general, only private IP addresses assigned through ITS from the 172.X.X.X range will be routed through the WAN. Agencies may also choose to use non-routable private IP addresses from the 10.X.X.X or 192.X.X.X ranges. Agencies that use private IP addresses for their local personal computers, workstations, and printers may choose to implement NAT (network address translation) for those devices that need access to the Internet. ITS will not automatically provide NAT for all privately assigned IP addresses. ITS will evaluate the need for NAT based on agency or service requirements. Agencies are encouraged to consider the use of private IP addresses for their local area networks where appropriate. Members of the ITS Review Team will be available to answer questions about implementing private IP addressing in agency LANs.

Service Delivery Process

This design provides a future direction that can be followed throughout the State Wide Area Network. Assignment and control of IP addresses and the VLAN numbering scheme will be the responsibility of

the Transport Planning group. The plan provides for future scalability because of the flexible way in which the numbering scheme has been designed. IPv6 and other changes to network configurations may change the numbering schemes in the above document. These types of changes will be evaluated as they are brought to light and plans will be put in place to provide the agencies with the best possible solutions that will provide all WAN participants with as much security, scalability, and flexibility as possible.

Appendix A – IP Assignments

Part One – Routed Private IP Ranges Assigned by Geographic Hub

Range	Mask	Octets	Area	Description
172.16.0.0	**255.255.0.0**	**256**	Here (SOB)	
172.17.0.0	255.255.128.0	128	Geographic Hub area 1	Cedar City
172.17.128.0	255.255.128.0	128	Geographic Hub area 2	Gunnison
172.18.0.0	255.255.128.0	128	Geographic Hub area 3	Logan
172.18.128.0	255.255.128.0	128	Geographic Hub area 4	Monticello (combined w/ Price)
172.19.0.0	**255.255.0.0**	**256**	Geographic Hub area 5	ORC
172.20.0.0	255.255.128.0	128	Geographic Hub area 6	So. Ogden (UHP)
172.20.128.0	255.255.128.0	128	Geographic Hub area 7	Price
172.21.0.0	**255.255.0.0**	**256**	Geographic Hub area 8	PRC
172.22.0.0	**255.255.0.0**	**256**	Geographic Hub area 9	Richfield (DOT)
172.23.0.0	255.255.128.0	128	Geographic Hub area 10	SLC#1 Heber Wells
172.23.128.0	255.255.128.0	128	Geographic Hub area 11	SLC#2 Cannon Health
172.24.0.0	255.255.128.0	128	Geographic Hub area 12	SLC#3 DHS Main
172.24.128.0	255.255.128.0	128	Geographic Hub area 13	SLC#4 Calvin Rampton
172.25.0.0	255.255.128.0	128	Geographic Hub area 14	SLC#5 USOR Murray
172.25.128.0	255.255.128.0	128	Geographic Hub area 15	St. George (Dixie College)
172.26.0.0	255.255.128.0	128	Geographic Hub area 16	Summit County
172.26.128.0	255.255.128.0	128	Geographic Hub area 17	Tooele County
172.27.0.0	255.255.128.0	128	Geographic Hub area 18	Vernal
172.27.128.0	255.255.128.0	128	Geographic Hub area 19	Wasatch County

Note: Other Private IPs will not be routed through the State WAN.

Part Two – Public IP Ranges for Agency Use

ITS will continue to assign public IP addresses to agencies from the available class B IP blocks that ITS owns and controls. These include:

168.177.0.0
168.178.0.0
168.179.0.0
168.180.0.0

Part Two – ITS Management VLAN 3

IP selected the following public IP range to use for ITS Management VLAN 3 subnets:

161.119.128.0 thru 161.119.191.254

Appendix B – VLAN Numbering Model for Agencies

STATE OF UTAH VLAN STANDARD NUMBERING PLAN FOR WAN

AGENCY	RANGE OF VLAN NUMBERS ASSIGNED TO AGENCY	VLANS IDENTIFIED FOR SPECIFIC USE	WHAT VLAN WILL BE USED FOR
ITS - INFORMATION TECHNOLOGY SERVICES	3-19	3	Managing ITS Owned Equipment
		4-18	For ITS Use
		19	WAN Wireless bridged VLAN
HUMAN SERVICES	20-29	20	Combined Desktop/ Server Network
		21	Desktop/ Workstation/ Printer/ Laptop Network
		22	Internal Servers Network (not accessed by Public)
		23	External Servers Network (Web Servers, etc. open to public)
		24-29	Reserved for Agency Use
RESERVE FOR ITS	30-39	30	Combined Desktop/ Server Network
		31	Desktop/ Workstation/ Printer/ Laptop Network
		32	Internal Servers Network (not accessed by Public)
		33	External Servers Network (Web Servers, etc. open to public)
		34-39	Reserved for Agency Use
WFS - WORK FORCE SERVICES	40-49	40	Combined Desktop/ Server Network
		41	Desktop/ Workstation/ Printer/ Laptop Network
		42	Internal Servers Network (not accessed by Public)
		43	External Servers Network (Web Servers, etc. open to public)
		44-49	Reserved for Agency Use
DOH - DEPARTMENT OF HEALTH	50-59	50	Combined Desktop/ Server Network
		51	Desktop/ Workstation/ Printer/ Laptop Network
		52	Internal Servers Network (not accessed by Public)
		53	External Servers Network (Web Servers, etc. open to public)
		54-59	Reserved for Agency Use
TAX COMMISSION	60-69	60	Combined Desktop/ Server Network
		61	Desktop/ Workstation/ Printer/ Laptop Network
		62	Internal Servers Network (not accessed by Public)
		63	External Servers Network (Web Servers, etc. open to public)
		64-69	Reserved for Agency Use

PUBLIC SAFETY	70-79	70	Combined Desktop/ Server Network
		71	Desktop/ Workstation/ Printer/ Laptop Network
		72	Internal Servers Network (not accessed by Public)
		73	External Servers Network (Web Servers, etc. open to public)
		74-79	Reserved for Agency Use
UDOT - UTAH DEPT OF TRANSPORTATION	80-89	80	Combined Desktop/ Server Network
		81	Desktop/ Workstation/ Printer/ Laptop Network
		82	Internal Servers Network (not accessed by Public)
		83	External Servers Network (Web Servers, etc. open to public)
		84-89	Reserved for Agency Use
DEPT OF ADMIN SERVICES	90-99	90	Combined Desktop/ Server Network
		91	Desktop/ Workstation/ Printer/ Laptop Network
		92	Internal Servers Network (not accessed by Public)
		93	External Servers Network (Web Servers, etc. open to public)
		94-99	Reserved for Agency Use
AGRICULTURE	100-109	100	Combined Desktop/ Server Network
		101	Desktop/ Workstation/ Printer/ Laptop Network
		102	Internal Servers Network (not accessed by Public)
		103	External Servers Network (Web Servers, etc. open to public)
		104-109	Reserved for Agency Use
ALCOHOLIC BEVERAGE CONTROL	110-119	110	Combined Desktop/ Server Network
		111	Desktop/ Workstation/ Printer/ Laptop Network
		112	Internal Servers Network (not accessed by Public)
		113	External Servers Network (Web Servers, etc. open to public)
		114-119	Reserved for Agency Use
ATTORNEY GENERAL	120-129	120	Combined Desktop/ Server Network
		121	Desktop/ Workstation/ Printer/ Laptop Network
		122	Internal Servers Network (not accessed by Public)
		123	External Servers Network (Web Servers, etc. open to public)
		124-129	Reserved for Agency Use
AUDITOR	130-139	130	Combined Desktop/ Server Network
		131	Desktop/ Workstation/ Printer/ Laptop Network
		132	Internal Servers Network (not accessed by Public)
		133	External Servers Network (Web Servers, etc. open to public)
		134-139	Reserved for Agency Use

BOARD OF PARDONS	140-149	140	Combined Desktop/ Server Network
		141	Desktop/ Workstation/ Printer/ Laptop Network
		142	Internal Servers Network (not accessed by Public)
		143	External Servers Network (Web Servers, etc. open to public)
		144-149	Reserved for Agency Use
BOARD OF REGENTS	150-159	150	Combined Desktop/ Server Network
		151	Desktop/ Workstation/ Printer/ Laptop Network
		152	Internal Servers Network (not accessed by Public)
		153	External Servers Network (Web Servers, etc. open to public)
		154-159	Reserved for Agency Use
COMMERCE	160-169	160	Combined Desktop/ Server Network
		161	Desktop/ Workstation/ Printer/ Laptop Network
		162	Internal Servers Network (not accessed by Public)
		163	External Servers Network (Web Servers, etc. open to public)
		164-169	Reserved for Agency Use
DEPT OF COMMUNITY & ECON DEV (DCED)	170-179	170	Combined Desktop/ Server Network
		171	Desktop/ Workstation/ Printer/ Laptop Network
		172	Internal Servers Network (not accessed by Public)
		173	External Servers Network (Web Servers, etc. open to public)
		174-179	Reserved for Agency Use
DEPT OF CORRECTIONS (DOC)	180-189	180	Combined Desktop/ Server Network
		181	Desktop/ Workstation/ Printer/ Laptop Network
		182	Internal Servers Network (not accessed by Public)
		183	External Servers Network (Web Servers, etc. open to public)
		184-189	Reserved for Agency Use
COURT ADMINISTRATORS	190-199	190	Combined Desktop/ Server Network
		191	Desktop/ Workstation/ Printer/ Laptop Network
		192	Internal Servers Network (not accessed by Public)
		193	External Servers Network (Web Servers, etc. open to public)
		194-199	Reserved for Agency Use
CRIME VICTIM REPARATIONS	200-209	200	Combined Desktop/ Server Network
		201	Desktop/ Workstation/ Printer/ Laptop Network
		202	Internal Servers Network (not accessed by Public)
		203	External Servers Network (Web Servers, etc. open to public)
		204-209	Reserved for Agency Use

SCHOOL OF DEAF AND BLIND	210-219	210	Combined Desktop/ Server Network
		211	Desktop/ Workstation/ Printer/ Laptop Network
		212	Internal Servers Network (not accessed by Public)
		213	External Servers Network (Web Servers, etc. open to public)
		214-219	Reserved for Agency Use
EDUCATION (USOE)	220-229	220	Combined Desktop/ Server Network
		221	Desktop/ Workstation/ Printer/ Laptop Network
		222	Internal Servers Network (not accessed by Public)
		223	External Servers Network (Web Servers, etc. open to public)
		224-229	Reserved for Agency Use
ENVIRONMENTAL QUALITY (DEQ)	230-239	230	Combined Desktop/ Server Network
		231	Desktop/ Workstation/ Printer/ Laptop Network
		232	Internal Servers Network (not accessed by Public)
		233	External Servers Network (Web Servers, etc. open to public)
		234-239	Reserved for Agency Use
FLEET OPERATIONS	240-249	240	Combined Desktop/ Server Network
		241	Desktop/ Workstation/ Printer/ Laptop Network
		242	Internal Servers Network (not accessed by Public)
		243	External Servers Network (Web Servers, etc. open to public)
		244-249	Reserved for Agency Use
FINANCE	250-259	250	Combined Desktop/ Server Network
		251	Desktop/ Workstation/ Printer/ Laptop Network
		252	Internal Servers Network (not accessed by Public)
		253	External Servers Network (Web Servers, etc. open to public)
		254-259	Reserved for Agency Use
FINANCIAL INSTITUTIONS	260-269	260	Combined Desktop/ Server Network
		261	Desktop/ Workstation/ Printer/ Laptop Network
		262	Internal Servers Network (not accessed by Public)
		263	External Servers Network (Web Servers, etc. open to public)
		264-269	Reserved for Agency Use
HUMAN RESOURCES MANAGEMENT (DHRM)	270-279	270	Combined Desktop/ Server Network
		271	Desktop/ Workstation/ Printer/ Laptop Network
		272	Internal Servers Network (not accessed by Public)
		273	External Servers Network (Web Servers, etc. open to public)
		274-279	Reserved for Agency Use

INDUSTRIAL COMMISSION	280-289	280	Combined Desktop/ Server Network
		281	Desktop/ Workstation/ Printer/ Laptop Network
		282	Internal Servers Network (not accessed by Public)
		283	External Servers Network (Web Servers, etc. open to public)
		284-289	Reserved for Agency Use
INSURANCE DEPT	290-299	290	Combined Desktop/ Server Network
		291	Desktop/ Workstation/ Printer/ Laptop Network
		292	Internal Servers Network (not accessed by Public)
		293	External Servers Network (Web Servers, etc. open to public)
		294-299	Reserved for Agency Use
LEGISLATURE	300-309	300	Combined Desktop/ Server Network
		301	Desktop/ Workstation/ Printer/ Laptop Network
		302	Internal Servers Network (not accessed by Public)
		303	External Servers Network (Web Servers, etc. open to public)
		304-309	Reserved for Agency Use
UTAH NATIONAL GUARD	310-319	310	Combined Desktop/ Server Network
		311	Desktop/ Workstation/ Printer/ Laptop Network
		312	Internal Servers Network (not accessed by Public)
		313	External Servers Network (Web Servers, etc. open to public)
		314-319	Reserved for Agency Use
DEPT OF NATURAL RESOURCES (DNR)	320-329	320	Combined Desktop/ Server Network
		321	Desktop/ Workstation/ Printer/ Laptop Network
		322	Internal Servers Network (not accessed by Public)
		323	External Servers Network (Web Servers, etc. open to public)
		324-329	Reserved for Agency Use
OFFICE OF REHABILITATION (USOR)	330-339	330	Combined Desktop/ Server Network
		331	Desktop/ Workstation/ Printer/ Laptop Network
		332	Internal Servers Network (not accessed by Public)
		333	External Servers Network (Web Servers, etc. open to public)
		334-339	Reserved for Agency Use
OFFICE OF PLANNING/ BUDGETING (OPB)	340-349	340	Combined Desktop/ Server Network
		341	Desktop/ Workstation/ Printer/ Laptop Network
		342	Internal Servers Network (not accessed by Public)
		343	External Servers Network (Web Servers, etc. open to public)
		344-349	Reserved for Agency Use

PUBLIC SERVICE COMMISSION (PSC)	350-359	350	Combined Desktop/ Server Network
		351	Desktop/ Workstation/ Printer/ Laptop Network
		352	Internal Servers Network (not accessed by Public)
		353	External Servers Network (Web Servers, etc. open to public)
		354-359	Reserved for Agency Use
TREASURER	360-369	360	Combined Desktop/ Server Network
		361	Desktop/ Workstation/ Printer/ Laptop Network
		362	Internal Servers Network (not accessed by Public)
		363	External Servers Network (Web Servers, etc. open to public)
		364-369	Reserved for Agency Use
TRUST LANDS	370-379	370	Combined Desktop/ Server Network
		371	Desktop/ Workstation/ Printer/ Laptop Network
		372	Internal Servers Network (not accessed by Public)
		373	External Servers Network (Web Servers, etc. open to public)
		374-379	Reserved for Agency Use
UTAH EDUCATION NETWORK (UEN)	380-389	380	Combined Desktop/ Server Network
		381	Desktop/ Workstation/ Printer/ Laptop Network
		382	Internal Servers Network (not accessed by Public)
		383	External Servers Network (Web Servers, etc. open to public)
		384-389	Reserved for Agency Use
NON-STATE AGENCIES	500-550		

Appendix C – VLAN Numbering Model for Services and Applications

VLAN ASSIGNMENTS BY SERVICE TYPE

TYPE OF SERVICE	VLAN #	
Omnilink IP Mobile Net	911	
Wireless Access Point Service	802	Native VLAN
8021 - 8029 = SSID	8021-8029	VLANs for SSID
8210 - 8216 = SSID	8210-8216	VLANs for SSID